ABSTRACT

Management of ciphertext devaluation in public key infrastructure is addressed by providing system and method using a certificate having a validity dependent on the amount of ciphertext associated with the certificate, i.e. a ciphertext limited certificate (CLC). Thus when the amount of ciphertext reaches or exceeds a predetermined value, the certificate is invalid. The CCE may be expressed as a non critical extension to a X.509 certificate to allow for interoperability with conventional validity conditions based on validity period or revocation. Ciphertext limited certificates may be implemented in an X.509 standard environment based on a method of assigning and determining a certificate ciphertext entitlement (CCE), calculating a generated Ciphertext index (CGI) and performing a CCE threshold detection, and when the GCI reaches or exceeds the CCE, causing a key update, e.g. a rollover of the certificate. Assurance levels may be set based on assigning different CCE default values.